People’s Role in Cyber Security: Academics’ Perspective

White Paper by Crucial Research
September, 2014

Introduction: Cyber Security is Everyone's Responsibility

Cyber threats are still one of the greatest concerns of the contemporary society. The fear of privacy or security breaches that has been dominant over the last few years has only grown with the recent celebrity photo leaks from iCloud. A major issue with this breach is that it has once again proved that security is not a concern for security specialists and enterprise ecosystems only. It is a menace anyone should learn to protect from.

With the events such as the breach of users' private photos (in this case female celebrities' nude photos), it is clear that nobody's data is safe on the web. One thing that seems to be a crucial issue here is the fact that internet users tend to rely on technology to protect them, while they also carry a significant degree of responsibility in this game.

People have grown to believe that advancements in technology are the only factor that guarantees their safety, but this view is obviously erroneous. Even though large organizations typically dedicate more attention to security regulations, the breaches often appear inevitable. No matter how much time and money a company invests into security systems implementation, breaches seem to keep occurring. One of the reasons for this is that nothing, not even in the age of technology boom can replace - people.

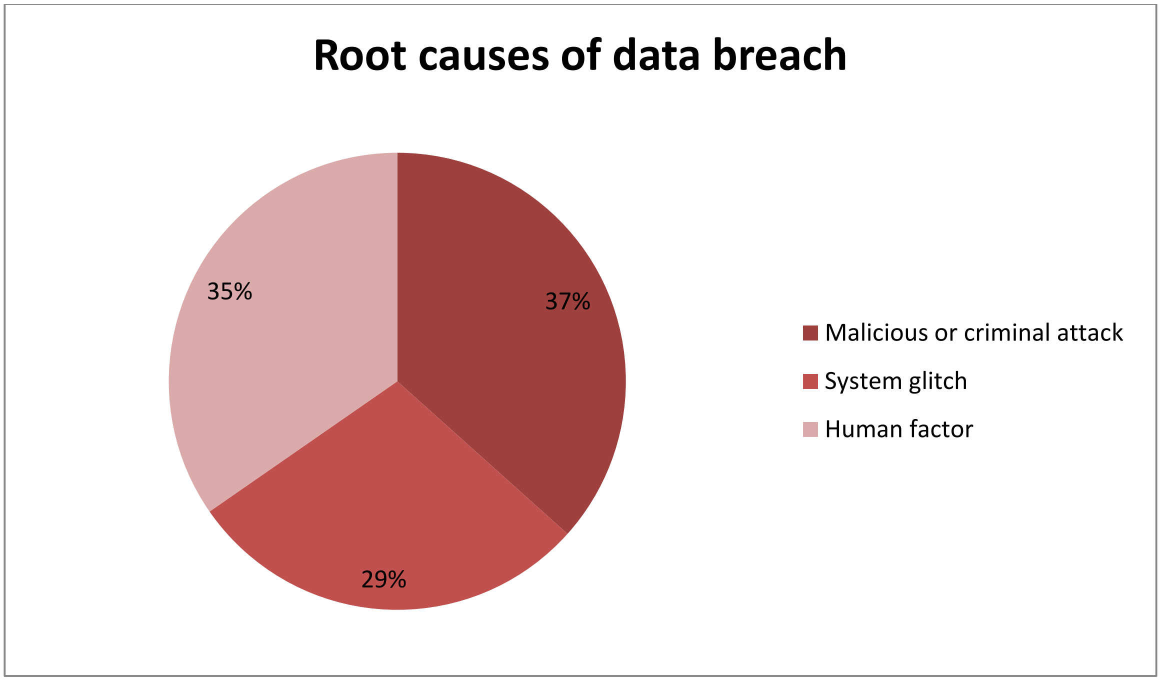
With an aim of emphasizing the role of people in computer and internet security, the Crucial research team presents the views of some of the major security specialists from prestigious U.S., U.K. and Australian Universities. Hopefully, these views will encourage internet users worldwide to start taking their privacy more seriously.

Human Factor in Computer and Internet Security: A Brief History

Five years ago, researchers at the University of Winsconsin-Madison (http://www.wisc.edu/) and IT University of Copenhagen (http://www.wisc.edu/) warned that people-related errors were the major factors in computer and internet security. They also noted that the problem was not likely to go away. Back then, they were analyzing MySpace password usage, which led them to conclude that the most commonly used password among MySpace users is – "password."

In 2014, SplashData's annual *Worst Passwords* list announced that this one finally went to the second place of their infamous list, only to be replaced by "123456." This is certainly an alarming finding for the world that currently counts 2,802,478,934 web users.

However, an even more alarming fact is that human error is still one of the most frequent causes of security breaches in corporate settings. This is a finding from Ponemon Institute's *2013 Cost of Data Breach Study: Global Analysis,* which confirms that human error is almost as frequent a cause for data breach as malicious and criminal attacks.



Source: Ponemon Institute: 2013 Cost of Data Breach: Global Analysis

The report makes it clear that people's role remains an significant factor in cyber security discussions. However, the way people use security systems is an often overlooked aspect of security regulations implementation in large organizations. One thing is for sure, though – both individual and professional users need to start taking their passwords seriously.

Good Users do Bad Things: Security in Theory and Practice

As pointed out in a research paper crafted by Jim Blythe from University of Southern California (http://www.usc.edu/), Ross Koppel from University of Pennsylvania (http://www.upenn.edu/) and Sean W. Smith from Dartmouth College (http://dartmouth.edu/), there is a great discrepancy between how security regulations work in theory and in practice.

Namely, the research suggests that despite the fact that security systems require people to use unique and strong passwords and keep them on a safe place, people are still finding the ways to circumvent and use security regulations in their organizations. Thus, we regularly see people who keep passwords on sticky notes on monitors and keyboards, or share them with friends to get their jobs done quickly.

Therefore, what actually happens in organizations does not usually match the expectations of security specialists. While IT specialists insist on regulations in password behavior, people still intentionally or unintentionally open doors to breaches in security systems, trying to make their lives easier. This fact calls for more education on this side of security process, as well as for security regulations that match real-world demands. As pointed out in the above mentioned scholars' article *Circumvention of Security: Good Users Do Bad Things:*

"According to folklore, after Galileo denied under duress that the Earth rotated around the sun; he then admitted, "and yet it moves." We feel similarly about cybersecurity and circumvention: it's ubiquitous, and we should stop pretending it's not."

People-Related Issues in Computer and Internet Security

Even though computer systems are nowadays immensely powerful, the role of people in managing security systems hasn't changed a lot. They still remain a crucial factor in ensuring maximum safety of their personal or corporate data. In support of this claim, Asgarkhani and Sitnikova from University of South Australia (http://www.unisa.edu.au/) made a list of people-related issues that directly impact their organizations' safety.

- **Lack of understanding and awareness** of implications of security compromises
- **A relaxed culture** where system reliability is not taken seriously
- **Lack of training for admin staff** so they can understand functions and risk implications
- **Lack of management training** to be aware of value of security and cost of being exposed to risks to their businesses
- **Shortage of suitability trained and skilled technical staff** who manage the operations of the system
- **An environment** where teamwork is not encouraged
- **Cultural differences** in multicultural environments where culture crashes may also result in teams not working together towards shared outcomes.

These may be seen as the primary causes of inadequate people's behavior when it comes to security systems at workplace. Unsurprisingly, many employees neglect their own role in maintaining security systems and protecting sensitive data. This is particularly dangerous in the era when the rise of cloud computing, expansion of VPS and adoption of mobile devices in corporate settings is booming, thus making data security a highly complex field.

Who are the Threats?

Hackers

Clearly, black-hat hackers are by far the biggest threat for the cyber space's well-being. Usually, their targets are smaller organizations, whom they attack with a goal of taking money, or just for the sake of making a prank. It is important to note, however, that not all hackers are created equal, meaning that not all of them work to harm other people. Nevertheless, many hackers do perform some serious crimes and are using sophisticated technology that is able to disrupt even the most advanced systems.

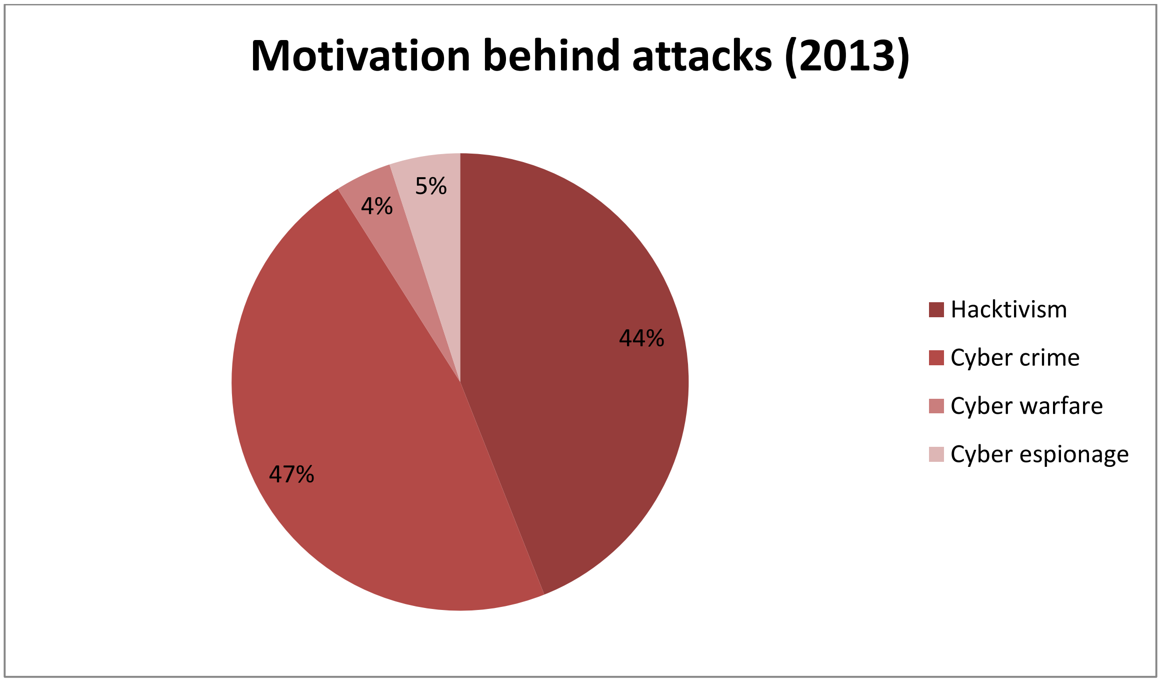
Another important thing is that there is a great variety of hacking practices, all of which have to be understood in order to get a clear picture of what is going on in cyber crime. Craig Webber, a senior lecturer in Criminology at University of Southampton (http://www.southampton.ac.uk/), points out that people should be a bigger focus of security discussions:

"Making more secure systems ignores the fact that cybercrime is based on trust, as in any criminal (and non-criminal) enterprise. Human intelligence of cybercrime networks and the ability to disrupt trust is just as important as the continual need to improve technological security" (Shades of Deviance 97)

Hacktivists

This subgroup of hackers, as many experts argue, is a rising threat to data safety on the Internet. David Turns, a senior lecturer at Cranfield University (http://www.cranfield.ac.uk/), defines hackers as "*people who are not part of their State's armed forces but on their own initiative carry out attacks against perceived 'enemy' computer systems, without the authority and outside the control of their government but in pursuance of common political ends."*

Hacktivism, correspondingly, is a type of cyber crime that involves politically-motivated attacks, frequently against targetted countries, and it has been growing significantly over the last few years. Last year, a report presented at Hackmageddon.com has graphically illustrated motivation behind cyber attacks.



Source: *Hackmageddon.com*

Social engineers

Social engineering has been a dominant form of tricking people into disclosing sensitive data, especially in small-to-medium-sized businesses. The phenomenon of social engineers is associated with people who intentionally build relationships with the employees in a particular organization, only to eventually obtain corporate data.

The university of Pennsilvania's (http://www.upenn.edu/) *Desktop Security 101: A Quick Course In Safer Computing* gives a witty definition of social engineers:

"Social engineering" is a term that has come into use in the computer security field over the last few years to describe the activities of what are, essentially, con men (and women). Their game is to get someone to willingly give them privileged information by exploiting some combination of:

A) The innate, good-natured desire to be of help to a fellow human being.
B) The belief that everyone basically honest.
C) The person's current state of being extremely busy and distracted.
D) The belief that bad things happen only to other people.
E) Stupidity.
F) All of the above.

Social engineering, therefore, represents another instance of how people can bring their or their organizations' data security in danger. Although most people are aware of the threats that could result from such a misuse of corporate data, social engineering still seems to be a frequent source of data leakage.

Who are the Hopes for Defense?

When discussing the ways safety on the web could be improved, the first thing that may pop up in one's mind is the introduction of stable technologies that would regulate data flow. However, educating people on the importance of this issue may bring even more beneficial results than secure hosting, especially when it comes to large organizations. The more the younger generations are familiar with the ways they could be protected on the Internet, the greater the chances of achieving stability in cyber space. Let us then have a look at the people who should be everybody's role models.

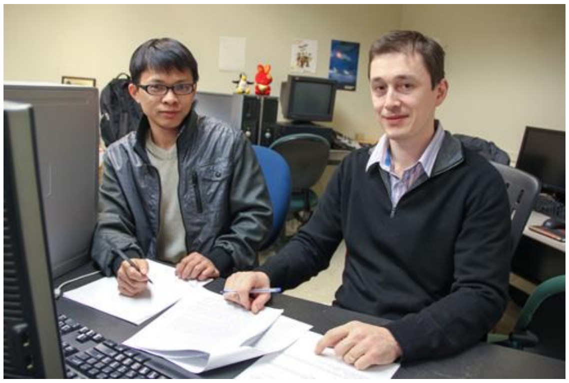
High-Shool Cyber Patriots

This is the idea behind CyberPatriot, a national high school cyber-defense competition sponsored by the Air Force Association. This competition encourages high school students to use cyber-defense systems, and potentially get scholarships for studying in the field. This is the case with Colin Mahns, a former student of Red Bank Regional High School teacher, who is behind the CyberPatriot competition. He is now a student at the New Jersey Institute of Technology (http://www.njit.edu) and is doing an internship at CBS in Manhattan.

Young Researchers

Furthermore, NJIT researchers Reza Curtmola and Bo Chen last year received a top honor for their work on improving security of data stored at potentially untrusted cloud storage providers. In the paper titled *Towards Self-Repairing Replication-Based Storage Systems Using Untrusted Clouds* they propose a new data management paradigm in which data owner is able to outsource both storage space and data management.

"Computer security today is on everyone's mind and we take our mission seriously at NJIT to get the word out so that computing can be safer and easier for everyone—whether people are trying to protect banking accounts or military secrets. This is an enormous growth area in research and education," says James Geller, the dean at College of Computing Sciences.



Conclusions

Data protection, especially in corporate settings, has always been a subject of much thought. Technology progress that brought about a variety of web-based systems has forced more pieces of data to take digital forms. Correspondingly, data protection systems have also become more automated, more technology-dependent and, perhaps more importantly, more web-based.

It is true that the proliferation of online systems for both data storage and protection has facilitated many everyday and professional activities. However, the role of people has not changed too much in comparison to more traditional settings. In fact, people remain the decision-makers when it comes to both choosing and implementing security systems, as well as in maintaining secure data flow. As pointed out by the academics quoted in this paper, security systems cannot guarantee protection as long as people are neglecting their parts of this immensely important responsibility.

References:

2013 Cyber Attacks Statistics (Summary). Hacmageddon.com. Available at: http://hackmageddon.com/2014/01/19/2013-cyber-attacks-statistics-summary/

The 2013 list of worst passwords. SplashData. Available at: http://splashdata.com/press/worstpasswords2013.htm

Asgarkhani and Sitnikova. Unisa. "A Strategic Approach to Managing Security in SCADA Systems." *13th European Conference on Cyber Warfare and Security, University of Piraeus,*

2014. Available at:
http://www.academia.edu/7665555/13th_European_Conference_on_Cyber_Warfare_and_Security_University_of_Piraeus_2014

Blythe, Jim, Ross Koppel and Sean W. Smith. *Circumvention of Security: Good Users Do Bad Things.* Available at: http://www.cs.dartmouth.edu/~sws/pubs/bks13.pdf

CyberPatriots hail from Red Bank teacher’s class. App.com. Available at:
http://www.app.com/story/news/education/in-our-schools/2014/08/22/cyberpatriots-hail-red-bank-teachers-class/14474687/

People are Still the Weakest Link in Computer and Internet Security, Study Finds. Science Daily. October, 14. 2009. Available at:
http://www.sciencedaily.com/releases/2009/10/091013110053.htm

Turns, David. *Journal of Conflict and Security Law.* Oxford University Press, 2012. Available at:
https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Turns.pdf

Webber, Craig. “Hackers and Cybercrime.” *Shades of Deviance: A Primer on Crime Deviance and Social Harm.* Ed. Atkinson, Rowland. New York: Routledge, 2014.

Web Hosting Security 2014. Whitepaper by Crucial.com.au. Available at:
http://www.crucial.com.au/blog/2014/07/30/whitepaper-web-hosting-security-2014/